LARA LICENSING AND REGULATORY AFFAIRS CUSTOMER DRIVEN. BUSINESS MINDED.	**Effective Date:**	09-12-2011
	Policy #:	G-18
	Supersedes:	**2004**

Subject: **Information Privacy and Security Breach Notification**	**Page:**	1 of 2

POLICY

This policy may be referenced to decrease the risk of loss of sensitive data using stolen department information. The policy offers procedures for when the loss of sensitive data is either reported or suspected to have occurred.

This policy and procedure is established consistent with the Identity Theft Protection Act (Public Act 452 of 2004). Specific attention is paid to information maintained electronically and accessible over the Internet.

DEFINITIONS

Information Security Event or Information Security Incident - Any event that is known or suspected to have compromised the confidentiality, integrity, or availability of department computer systems, networks, data, or records. Only the IPO may declare an incident.

Sensitive - Records intended for limited internal use within the department that, if disclosed, could be expected to have a severe adverse effect on the operations, assets, or reputation of the department or its obligations concerning information privacy. Sensitive data may include data connecting a person's name with the person's (a) social security or driver's license number, (b) medical information, (c) financial information, or (d) other information designated as sensitive by the Privacy Council. The release or disclosure of sensitive data should only occur consistent with existing redaction, de-identification, and other privacy policies.

PROCEDURE

Responses to Loss of Sensitive Data

Preliminary response to a reported or potential loss of sensitive data should occur as soon as possible, and in all cases within 12 hours of initial contact during regular business hours. Events reported after close of business should have a preliminary response by close of business the following day.

Following a suspected identity theft, an employee should contact the Information Privacy Officer (IPO) in the Director's Office to report the data suspected to have been compromised. The IPO will alert appropriate staff to initiate an investigation and may create an incident response team to initiate an investigation. Any team should coordinate its response under this policy with the Department IPO.

A response team shall begin a preliminary investigation immediately. If a breach of sensitive data has likely occurred, the team shall contact the IPO to ensure that a response plan is created. The IPO shall ensure that victims are (1) contacted once it is determined that an identity theft likely occurred and (2) shall provide an update regarding the status of the identity theft response and investigation. The IPO shall coordinate investigation with appropriate business, technical, security, and law enforcement resources.

Standards

After an investigation, the IPO shall review and amend processes and procedures as appropriate based on the investigation outcome. The IPO shall take appropriate steps to educate employees on strategies to minimize the risk of identity theft, including password protection and cyber security measures.

Risk assessments should be conducted regularly to identify and minimize potential exposure points. The IPO will coordinate with the Department of Technology Management and Budget, Office of Enterprise Security (DTMB-OES) to ensure that vulnerability scans and related remediation occur as scheduled. A response plan will be developed and revised as necessary that includes standard investigation steps, contact information, key staff, and standard preliminary information to provide victims. Information provided may include how to contact banks and credit card companies, actions being taken by the response team, and an anticipated communication schedule.